Vendor Management Policy

CHANGE HISTORY

Date	Version	Created by	Approved By	Description of change
08/10/2024	1.0	Bharath S	Ashwin Khosla	Basic document outline and submitted for review

Purpose

This policy defines the rules for relationships with the organization's Information Technology (IT) vendors and partners. The purpose of this policy is to ensure that risks associated with outsourced vendor relationships are minimized. As vendors' people, technologies, and practices evolve over time, Veranda Learning must ensure the appropriate levels of due care and due diligence are applied to validate that IT security controls are effective. The objective is to ensure the protection of the company's assets that is accessible by suppliers/vendors.

Scope

Vendor Management policy applies to the following:

- All vendors / third-party / visitors who temporarily access Veranda Learning information assets
- Software procured

Background

The overall security of the organization is highly dependent on the security of its contractual relationships with its IT suppliers and partners. This policy defines requirements for effective management and oversight of such suppliers and partners from an information security perspective. The policy prescribes minimum standards a vendor must meet from an information security standpoint, including security clauses, risk assessments, service level agreements, and incident management. Veranda Learning assesses vendors to determine if their IT security controls are effective. Veranda Learning also ensures that vendors implement mechanisms to identify and remediate deficiencies or vulnerabilities on an ongoing basis, in order to ensure the continued effectiveness of IT security controls.

Policy

All supplier relationships are vetted by the Information Security Council (ISC). Where possible, a written contract shall exist between all parties involved, and Veranda Learning will hold an original signed by all parties, which will be held electronically.

The contract will include the following items where possible:

- The scope of the services to be delivered.
- Dependencies between services, processes, and the parties
- Requirements to be fulfilled by the supplier
- Service targets
- Interfaces between service management processes operated by the supplier and other parties
- Integration of the supplier's activities within the Service Management System
- Workload characteristics
- Exceptions
- Authorities and responsibilities of Veranda Learning and the supplier
- Reporting and communication to be provided by the supplier
- Basis for charging
- Activities and responsibilities for the expected or early termination of the contract and the transfer of services to a different party
- The roles and relationships between lead and sub-contracted suppliers will be documented.

- Regular formal communication is made with suppliers on a frequency-dependent upon the amount of business conducted with the supplier and the importance of the goods or services to Veranda Learning.

Any changes to the scope or terms of existing contracts are managed and documented fully via the change management process. Contracts will be stored within the Company contracts file system to document details of the suppliers of IT goods and services to the company, including contacts, service levels, sub-contracted suppliers, and the main contract terms.

Supplier Information Security Requirements and Policy

In general, information security requirements will vary according to the contractual relationship that exists with each supplier. The selection of controls should be based upon a comprehensive risk assessment taking into account information security requirements, the product or service to be supplied, its criticality to the organization, and the supplier's capabilities.

However, the following will generally apply within the context of the supplier categories described in this policy.

- Access to Veranda Learning information should be limited to suppliers in the Tactical and Strategic categories.
- The information security requirements and controls should be formally documented in a contractual agreement that may be part of, or an addendum to, the main commercial contract.
- Separate Non-Disclosure Agreements should be used where more specific control over confidentiality is required.
- Remote access must be via approved methods that comply with our information security policies.
- Basic information security principles such as least privilege, separation of duties, and defense in depth should be applied.
- The supplier will be expected to exercise adequate control over the information security policies and procedures used within sub-contractors who play a part in the supply chain of delivery of goods or services to Veranda Learning.
- Veranda Learning will have the right to audit the information security practices of the supplier and, where appropriate, sub-contractors.
- Incident management and contingency arrangement should be put in place based on the results of the risk assessment.
- Security awareness training will be carried out by both parties to the agreement, based on the defined processes and procedures.

Appropriate legal advice must be obtained to ensure that contractual documentation is valid within the country(ies) in which it is to be applied.

Supplier Performance Management

The performance of strategic suppliers will be monitored on a regular basis in line with the recommended meeting frequency. This will take the form of a combination of supplier-provided reports against the contract and internally produced reports from the Engineering Team. Where possible, a frequent cross-check will be made between the supplier reports and those created via the Engineering Team to ensure the two present a consistent picture of supplier performance. Both sets of reports will be reviewed at supplier meetings and any actions resulting will be input into the Continual Improvement plan.

Contractual Disputes

In the event of a contractual dispute, the following guidelines should be followed:

- The CEO must be informed that a dispute exists.

- The CEO must be in agreement as to the next steps.
- Where applicable, legal advice should be obtained via the CEO.
- All correspondence with the supplier must be in writing.
- An assessment of the risk to the organization should be carried out prior to escalating any dispute, and contingency plans put in place.

At all times, the degree of risk to the business should be managed and if possible minimized.

End of Service

The following process will be followed for the end of service, the early end of service, or the transfer of service to another party:

- The end of service will be requested in writing within the terms of the contract if one exists.
- Transfer to another party (including in-house support) shall be planned via the Design and transition of a New or Changed Service process and change control procedures followed.
- An assessment of the risk to the organization should be carried out prior to ending or transferring the service, and contingency plans put in place.
- Any budgetary implications shall be incorporated into the financial model.

In line with this policy, the various aspects of ending a service should be carefully considered during the initial contract negotiation time.

Mapping with Industry Standards

This policy addresses the following risks related to supplier management and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Loss of CIA (confidentiality, Integrity, and Availability)	5.20 Addressing information security within supplier agreements 5.22 Monitoring, review and change management of supplier services
Unauthorized Use of Information assets	5.20 Addressing information security within supplier agreements
Non-adherence to the laws and regulations and Compliance	5.20 Addressing information security within supplier agreements 5.21 Managing information security in the ICT supply chain
Unauthorized access	5.20 Addressing information security within supplier agreements 5.19 Information security in supplier relationships
Information Leakage	5.19 Information security in supplier relationships 5.20 Addressing information security within supplier agreements 5.21 Managing information security in the ICT supply chain
Theft	5.19 Information security in supplier relationships

Risk	Mapping to ISO 27001:2022
	5.20 Addressing information security within supplier agreements

Enforcement

Information security department and procurement department are responsible for enforcing vendor management policy.
All departments must ensure compliance with the vendor management policy when procuring new software or contracting a new vendor for services.

Non- Compliance

Violations of the policy may subject employees to disciplinary action, including removal of privilege to the systems, up to and including termination of employment. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

- Disciplinary action according to applicable Veranda learning policies.
- Termination of employment.
- Legal action according to applicable laws and contractual agreements.

Validity and Document Management

The owner of this document is the management, who must check and, if necessary, update the document at least once every 12 months